STELLUNGNAHME

## Vorläufige Stellungnahme des eurobits e.V.

**zum „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“ des Bundesministeriums des Inneren für Bau und Heimat (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0); bezugnehmend auf den Diskussionsentwurf des BMI vom 09.12.2020, Referentenentwurf vom 21.11.2020**

Der eurobits e.V. – Europäisches Kompetenzzentrum für IT-Sicherheit begrüßt ausdrücklich den Entwurf des IT-SiG 2.0 und das damit verbundene Bekenntnis zum hohen Stellenwert der IT-Sicherheit seitens des Gesetzgebers. Aufbauend auf den durch das IT-Sicherheitsgesetz 1.0 erzielten Erfolgen setzt das IT-SiG 2.0 weitere wichtige Impulse und definiert verbindliche Regeln in einem Themenfeld von nicht zu unterschätzender Wichtigkeit: Zukünftige Wettbewerbsfähigkeit kann nur durch nachhaltige Digitalisierung gelingen. Digitalisierung muss sicher sein – in den privaten Haushalten, in der Wirtschaft (insbesondere bei KMU), den Kommunen und Behörden sowie in sämtlichen Kritischen Infrastrukturen (KRITIS).

Während eurobits den neuen Gesetzesentwurf in weiten Teilen uneingeschränkt befürwortet, sieht der Verein in folgenden Punkten noch dringenden bzw. zukünftigen Änderungsbedarf:

1. Der im Gesetz noch unzureichend beschriebene **„Stand der Technik“ als unbestimmter Rechtsbegriff muss besser definiert und vereinheitlicht werden.** Nur so kann jeder Betreiber nach einem einheitlichen hohen Sicherheitsniveau geprüft bzw. zertifiziert werden. (Ansätze für eine mögliche Vorgehensweise siehe 5.)
2. Der eurobits e.V. bewertet das IT-Sicherheitsgesetz 1.0 als Erfolg bei großen Betreibern, die KRITIS-Dienstleistungen für mehr als 500.000 zu versorgende Personen anbieten. Dieser **Schwellenwert** sollte zukünftig gesenkt werden, um kritische Dienstleistungen auch für kleinere Betreibereinheiten im Falle eines Cyberangriffes garantieren zu können. eurobits regt an, den entsprechenden Schwellenwert **auf 250.000 Personen** zu **senken**. Damit wären die KRITIS-Betreiber zahlreicher Städte und Regionen verpflichtet, ihre Systeme und IT-Infrastruktur entsprechend der gesetzlichen Anforderungen abzusichern und damit die Versorgungssicherheit zu erhöhen. Der eurobits e.V. empfiehlt zudem eine Evaluierung der umgesetzten Maßnahmen spätestens ein Jahr nach Inkrafttreten des Gesetzes.
3. Der deutliche **Ausbau des Angebots von Beratungsleistungen** zum Thema IT-Sicherheit innerhalb des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird vom Verein kritisch gesehen. Hier gilt es dringend sicher zu stellen, dass bereits existierende Marktangebote nicht beeinträchtigt werden. Um ein gesundes Öko-System und eine leistungsstarke nationale IT-Sicherheitsindustrie zu erhalten, sollte von der neu im IT-SiG formulierten vorgesehenen Beauftragung von Drittunternehmen deutlich Gebrauch gemacht werden. (BSIG §7a Abs.1)
4. Das IT-SiG 2.0 nimmt insbesondere hinsichtlich der, grundsätzlich von eurobits begrüßten, Stärkung des BSI angeht **keinen Bezug auf Aspekte der Regionalisierung**.

Dies widerspricht nach Auffassung des Vereins dem grundsätzlichen föderalen Prinzip der Bundesrepublik Deutschland. Hierdurch wird ein weiteres hochkritisches Element für Cybersicherheit zentral etabliert, statt auf ergänzende regionale Niederlassungen zu setzen, wie es bei anderen sicherheitsrelevanten Organen der Fall ist (bspw. BKA >> LKAs >> regionale und lokale Polizeidienststellen). Eine entsprechende regionale Organisationsform muss nach Auffassung des eurobits e.V. bereits im Gesetz verankert bzw. angedacht werden.
Andere Sicherheitsbehörden des Bundes haben entsprechende Spiegelbehörden in den Ländern und erhöhen demzufolge u.a. die Verfügbarkeit, Kompetenz und regionale Zuständigkeit. Daher sind Landes-Behörden auch für das Thema Cybersicherheit mit Zuständigkeit für die regionalen kritischen Infrastrukturen und Industrien zu fordern.

5. Der eurobits e.V. vermisst im Gesetzesentwurf die **Einbindung von Forschung und Wissenschaft** in wichtige Prozesse. Speziell Nordrhein-Westfalen hat sich im internationalen Vergleich als Cluster mit außerordentlich hoher IT-Sicherheits-Expertise etabliert und sich eine tadellose Reputation erarbeitet. Das an der Ruhr-Universität Bochum ansässige Horst-Görtz-Institut beispielsweise ist weltweit führend in der Zahl der veröffentlichten Beiträge zum Thema Cybersicherheit. Zahlreiche Hochschulen und andere Bildungsinstitute im bevölkerungsreichsten Bundesland liefern kontinuierlich wichtige Impulse und Erkenntnisse im Bereich Cybersicherheit und bilden die IT-Sicherheits-Experten von morgen aus. Diese Fachkompetenz sollten Gesetzgeber und Ministerien insbesondere bei der Analyse und Definition der im Gesetz genannten „kritischen Komponenten" sowie bei der Bestimmung des „Standes der Technik" nutzen. Ein erster Schritt in diese Richtung könnte z.B. die Berufung eines Beratungsgremiums sein, das u.a. mit Experten aus der IT-Sicherheitsbranche sowie mit Vertretern der Wissenschaft besetzt wird (ggf. auch unter Rückgriff auf ein bereits existierendes IT-Sicherheitsgremium). In einem solchen Gremium könnten zumindest Merkmale bzw. Bewertungskriterien für die Nutzung zukünftiger Technologien erarbeitet werden.
6. Der eurobits e.V. weist nachdrücklich darauf hin, dass sämtliche Bestimmungen und Vorschriften, die sich aus dem IT-SiG 2.0 ergeben, **auf europäischer Ebene abgestimmt** werden sollten. Nur so sind der nachhaltige Aufbau und Erhalt einer Cyber-Resilienz im internationalen Wettbewerb möglich. Eine enge Koppelung mit der gerade in Überarbeitung stehenden NIS-Richtlinie wird als zwingend erforderlich angesehen. eurobits plädiert außerdem nachdrücklich für eine Harmonisierung des IT-SiG 2.0 mit dem Cyber Security Act. Ebenfalls zweifelt eurobits an der Sinnhaftigkeit nationaler IT-Sicherheits-Siegel. Entsprechende Initiativen sollten immer auf europäischer Ebene angestrebt und umgesetzt werden. Generell wünscht sich der Verein ein in allen Punkten eng abgestimmtes Vorgehen zwischen dem BSI und der ENISA.
7. Für die Zukunft wünscht sich der eurobits e.V. seitens der verantwortlichen Stellen einen der Komplexität und Wichtigkeit des Themas angemessenen Zeitraum zur Analyse und Kommentierung entsprechender Gesetzesentwürfe. Eine wie in diesem Fall deutlich **zu kurz gesetzte Frist** von lediglich sieben Tagen ist nicht ausreichend für eine umfassende Analyse und abschließende Stellungnahme.

Abgesehen von den genannten Punkten begrüßt eurobits ausdrücklich folgende Aspekte des IT-SiG 2.0:

- Das neue Gesetz führt viele Ansätze des IT-Sicherheitsgesetzes 1.0 konsequent fort und erweitert diese wo nötig. Dies schätzt der Verein äußerst positiv ein, da bereits das erste Gesetz von 2015 nach Ansicht des eurobits e.V. ein Erfolg war und ist: Viele Betreiber Kritischer Infrastrukturen haben erfolgreich beispielsweise ein Informations-Sicherheits-Management-System (ISMS) eingeführt und damit neben den organisatorischen Voraussetzungen auch den Grad ihrer technischen IT- bzw. OT-Sicherheit in Infrastrukturen und Prozessen erhöht. Unsere Versorgung ist damit sicherer geworden.
- Die regulatorischen Eingriffe, die das IT-SiG 2.0 vorsieht, schaffen ein einheitliches IT-Sicherheitsniveau in Bereichen, die eine besondere Wichtigkeit haben. Dies schafft Sicherheit und faire Bedingungen für alle Marktteilnehmer. Regulierungen und Vorgaben aus der analogen Welt, beispielsweise beim Brandschutz, haben gezeigt, dass entsprechende Verordnungen notwendig sind, um Schäden von Bürgern und Wirtschaftsunternehmen abzuwenden. Dies gilt gleichermaßen für die digitale Welt.
- eurobits unterstützt insbesondere die Neuerungen im IT-SiG 2.0 in folgenden Bereichen:
    - Erweiterungen der KRITIS-Branchen (z.B. Siedlungsabfallwirtschaft)
    - Verpflichtungen von Herstellern u.a. zur sicheren Supply Chain
    - Erweiterungen Verbraucherschutz
    - Verpflichtender Einsatz von Systemen zur Angriffserkennung: Darin sieht eurobits einen wichtigen Schritt in Richtung proaktiver IT-Sicherheitslandschaft und zu einem Paradigma der „Prevention, Protection and Detection“. Auch der sinnvolle Transfer von Systemen zur Angriffserkennung in andere (Geltungs-)Bereiche wie §11 EnWG ist zu begrüßen.

  Diese Maßnahmen zahlen unmittelbar auf eine allgemeine Steigerung der IT-Sicherheit im Bundesgebiet ein und fördern so auch die langfristige Resilienz gegenüber Cyberattacken.

Ebenfalls begrüßt der Verein die Höhe der fälligen Bußgelder im Falle von Verstößen gegen das IT-SiG 2.0 – eine Anpassung an die DSGVO-Bußgeld-Höhe ist sinnvoll, da IT-Sicherheit in unserer heutigen Bedrohungslage ein immens wichtiges Gut ist.

- Aufgrund der bereits erwähnten sehr kurzen Frist versteht sich diese Stellungnahme als vorläufig und wird bei Bedarf in den kommenden Wochen oder bei substanziellen Änderungen am vorliegenden Diskussionsentwurf um weitere Punkte ergänzt bzw. an den entsprechenden Stellen geändert. Zusammenfassend betont der eurobits e.V. nochmals seine Unterstützung und die Notwendigkeit des neuen Gesetzes, vorbehaltlich der eingangs genannten konstruktiven Kritikpunkte.

# STELLUNGNAHME

**Über eurobits**

Der eurobits e.V. wurde 1999 gegründet und ist das europäische Kompetenzzentrum für Sicherheit in der Informationstechnologie mit Sitz in Bochum. Führende Forschungsinstitute, etablierte Unternehmen der Branche sowie junge Wachstumsunternehmen sind in einem europaweit einzigartigen Zusammenschluss integriert mit einem starken Fokus auf der Zusammenarbeit und dem Transfer zwischen Wirtschaft und Wissenschaft im Bereich IT-Sicherheit und Informationssicherheit.

Interdisziplinarität und die enge Verzahnung von Forschung und Anwendung zeichnen den eurobits e.V. aus. Die zentrale Idee des Vereins ist es, neben internationaler Spitzenforschung auf der Universitätsseite, eine exzellente Aus- und Weiterbildung sowie eine Umsetzung und Kommerzialisierung des enormen Know-hows durch Technologieunternehmen und Start-ups zu bewerkstelligen.

**Ansprechpartner für Rückfragen:**

Florian Szigat
Projektleiter eurobits e.V.

E-Mail: florian.szigat@eurobits.de
Telefon: +49 234 5457200-1

Postalische Adresse:

eurobits e.V.
Lise-Meitner-Allee 4
44801 Bochum